

Acercando la ciberseguridad a la escuela secundaria desde una perspectiva lúdica

Gabriela Suárez¹, Benjamín Freccero Starnari², Paula Venosa³, Claudia Queiruga⁴

¹ CERTUNLP (Centro de Respuestas de Incidentes de Seguridad Académico de la UNLP) - Argentina

^{2,3,4} LINTI (Laboratorio de Investigación en Nuevas Tecnologías Informática) - Facultad de Informática - UNLP - Argentina

gsuarez@cert.unlp.edu.ar, benjamin.freccero175916@alumnos.info.unlp.edu.ar, {pvenosa,claudiaq}@info.unlp.edu.ar

Resumen. En el presente trabajo se describe y analiza la experiencia de acercar la ciberseguridad a estudiantes de escuelas secundarias de la provincia de Bs As, Argentina, en el contexto del proyecto "Extensión en vínculo con escuelas secundarias" de la UNLP. Se analiza la relevancia de incorporar estos contenidos en la educación obligatoria, entendida como el ámbito fundamental de formación ciudadana, en donde se plantea como urgente la inclusión de contenidos del campo de la Informática (específicamente de ciberseguridad) en los diseños curriculares y a la vez que orienten una construcción de vocaciones profesionales. Existen experiencias locales y regionales que abordan la ciberseguridad en las escuelas, sin embargo, lo novedoso de esta propuesta es el enfoque adoptado: realizar eventos *Capture The Flag* orientados a escuelas secundarias del área de influencia de la UNLP, que permitan construir conocimiento de una manera lúdica. Se describen las experiencias y aprendizajes de los eventos realizados en clave de selección de contenidos, modalidad, conformación de los equipos y rol docente. Finalmente, se presentan los resultados obtenidos de encuestas realizadas a estudiantes y docentes, que revelan el interés de los estudiantes en continuar participando, y el interés de los docentes en la herramienta y la didáctica empleada.

Palabras claves: Ciberseguridad · Escuela Secundaria · Informática · Educación en Informática · Gamificación.

Received May 2024; Accepted June 2024; Published July 2024

Abstract This paper describes and analyzes the experience of bringing cybersecurity to secondary school students in the Buenos Aires province, Argentina, in the context of the UNLP project "Extension in connection with secondary schools". The relevance of incorporating these contents in compulsory education is analyzed, understood as the fundamental area of citizen education, where the inclusion of Information Technology (specifically cybersecurity) contents in curricular designs is proposed as urgent and at the same time guide a construction of professional vocations. There are local and regional experiences that address cybersecurity in schools, however, the novelty of this proposal is the approach adopted: holding Capture The Flag events aimed at secondary schools in the area of influence of the UNLP, which allow knowledge to be built in a playful methodology. The experiences and learnings from the events carried out are described in terms of content selection, modality, team formation and teaching role. Finally, the results obtained from student and teacher surveys are presented, which reveal the students' interest in continuing to participate, and the teachers' interest in the tool and the didactics used.

Keywords Cybersecurity · High School · Computer Science · Computer Education · Gamification.

1 Introducción

El trabajo aquí presentado forma parte del proyecto "Extensión en vínculo con escuelas secundarias"¹ de la UNLP, cuyo objetivo es discutir y dar a conocer la Informática como campo de conocimiento en la escuela secundaria, entendida ésta como una disciplina fuertemente vinculada al desarrollo socio-productivo y al campo laboral. Es en este último aspecto que desde el proyecto se llevan adelante prácticas educativas que colaboran en el proceso de construcción de una vocación o gusto por la Informática, a partir de la experiencia de comprender y vivenciar, entre otras cosas, cómo se construye un artefacto digital, cuáles son las implicancias de la huella digital, cómo se vinculan las vulnerabilidades de las aplicaciones (que usamos habitualmente) con la programación de las mismas, y no en la mera recepción de información descriptiva sobre los planes de estudio de las carreras. En este sentido concebimos la construcción de una vocación que pueda pensarse como un proyecto de vida, comprendiendo, fundamentalmente, las posibilidades de desarrollo profesional y de inserción laboral que ofrece la Informática en una sociedad donde las tecnologías digitales cobran un rol central, transformando la mayoría de las actividades de creación humana [1] [2]. La capacidad de saber usarlas, comprenderlas e intervenirlas se torna cada vez más relevante para la participación en la vida social, económica y política.

¹ Desde el año 2019 la UNLP comenzó a trabajar en programas de extensión (<https://www.extension.info.unlp.edu.ar/programa-de-extension-unlp/>). Bajo este marco, el equipo del proyecto "Extensión en vínculo con escuelas secundarias" integra el programa "Educación para la inclusión".

A su vez, a pesar de los avances en nuestro país sobre la introducción de contenidos de Informática en la escuela, el abordaje que prevalece en la mayoría de las escuelas de la provincia de Buenos Aires es el de "Informática de usuario", haciendo hincapié en el conocimiento y la capacidad de utilizar las computadoras y la tecnología relacionada con ellas, adoptando un enfoque "utilitario" en algunos casos, e "integrador" en otros [3], sin abordar las especificidades de la Informática como disciplina. Mencionamos esta jurisdicción dado que es el área de influencia del proyecto. En este sentido, podemos afirmar que la formación para el ejercicio de la ciudadanía ofrecida en nuestras escuelas, no atiende la educación en tecnologías digitales en el sentido de comprender cómo se construyen artefactos digitales, cómo funcionan realmente y qué implicancias tienen en la vida de las personas. Es por ello que la construcción de conocimiento sobre el campo de la Informática constituye un área de vacancia en la formación de nuestros jóvenes en el sistema de educación obligatoria y es en este sentido que el abordaje de la ciberseguridad cobra relevancia en el proyecto.

En este trabajo se propone la incorporación de desafíos o retos de ciberseguridad gamificados en competencias *Capture The Flag* (CTF), como metodología de enseñanza para acercar contenidos de ciberseguridad a la escuela.

2 Enseñar y aprender ciberseguridad en la escuela: ¿Para qué? ¿Cómo enseñarla? ¿Qué contenidos enseñar?

2.1 Relevancia de la ciberseguridad en la escuela: ¿para qué aprender sobre ciberseguridad?

La ciberseguridad es un área de conocimiento dentro del campo disciplinar de la Informática estrechamente vinculada a la protección de la información, de los servicios y las comunicaciones [4] [5]. A su vez, se relaciona con amenazas que ocurren en Internet, como el robo de información, la suplantación de identidad, el fraude digital, entre otras acciones. Las consecuencias de dichas acciones usualmente derivan pérdidas económicas, como así también en otros fenómenos relacionados con problemáticas sociales que afectan particularmente a los jóvenes como el *grooming*, el *sexting*, el *ciberbullying* cuando usan redes sociales y juegos en red. En relación a esta última cuestión, podemos afirmar que, en general, los niños y jóvenes no son conscientes de los riesgos que ocasiona la excesiva publicación de fotos, comentarios sensibles e información privada en las redes sociales. En este sentido, la adopción por parte de niños y jóvenes de estas tecnologías los expone a riesgos y amenazas en línea, y es en este aspecto que la formación en competencias en ciberseguridad favorece a la navegación segura en Internet y a la protección de la privacidad. Varias investigaciones, a nivel local, regional y global, dan cuenta de esta problemática desde el campo de la educación y también desde los gobiernos, poniendo en el centro de discusión la necesidad de educar en ciberseguridad desde edades tempranas [6] [7]. Por otra parte, desde el campo laboral, la demanda de profesionales y técnicos en

ciberseguridad, es otro aspecto a atender desde la educación, en relación a ofrecer una formación vinculada con el trabajo y la continuidad de los estudios. Según el informe de la OEA del 2023 [8] se estima que la escasez de profesionales en ciberseguridad en la región América Latina y el Caribe, oscila entre 515.000 y 701.000 personas. El mismo informe sostiene que los sistemas educativos representan un actor relevante, particularmente las escuelas, institutos y universidades, ofreciendo una formación que favorezca el desarrollo “[...] de una amplia gama de habilidades (habilidades de vida, habilidades blandas, habilidades técnicas y habilidades duras) para incursionar en el campo cibernético” (pp. 12). A nivel global, según el informe anual de la ISC2 Cybersecurity Workforce Study del 2022 la escasez de profesionales de ciberseguridad se estima en unos 3,4 millones de personas [9].

2.2 Estrategia de enseñanza: ¿cómo enseñar ciberseguridad?

Desde el proyecto “Extensión en vínculo con escuelas secundarias”, se acercan temas de ciberseguridad a los estudiantes de escuelas secundarias, a través de propuestas de resolución de desafíos o retos bajo la metodología conocida como *Capture The Flag* (CTF). Los retos se vinculan fundamentalmente a problemáticas relacionadas con la exposición de datos personales, no sólo en clave de sensibilizar y concientizar, sino fundamentalmente con la intención de introducirlos en un campo de conocimiento nuevo en relación a las tecnologías digitales, que va más allá del uso de las mismas. A su vez, aprender y descubrir en la ciberseguridad un vasto campo de la Informática con fuerte vinculación con el ámbito laboral, es también un propósito del proyecto.

La gamificación es un concepto estrechamente relacionado con los juegos digitales y se refiere al “uso de elementos del diseño de juegos en contextos no lúdicos” [10, pp. 9]. Para [11] “Gamificar es plantear un proceso de cualquier índole como si fuera un juego. Los participantes son jugadores y como tales son el centro del juego, y deben sentirse involucrados, tomar sus propias decisiones, sentir que progresan, asumir nuevos retos, participar en un entorno social, ser reconocidos por sus logros y recibir retroalimentación inmediata. En definitiva, deben divertirse mientras consiguen los objetivos propios del proceso gamificado”. En este sentido, el uso de elementos propios de los juegos en contextos que no son puramente de entretenimiento, como el educativo, busca mejorar la motivación y la participación de los estudiantes, dado que facilita la interiorización de conocimientos de una forma entretenida, generando una experiencia de aprendizaje positiva. Esto se puede llevar a cabo mediante diferentes actividades, como la resolución de problemas, el alcance de objetivos, el trabajo en equipo, entre otras. En [12] identifican el aburrimiento, la alienación y la desconexión entre las actividades de aprendizaje y la aplicación de los conocimientos en la vida real, como los motivos de la falta de involucramiento de los estudiantes con el aprendizaje. En este sentido, la gamificación enfoca a los estudiantes en los contenidos relevantes, proporciona retroalimentación oportuna que mejora la retención y soporta múltiples estilos de aprendizaje [13].

2.3 Temas de ciberseguridad a abordar en la escuela: ¿qué contenidos?

Los programas de ciberseguridad de cursos universitarios se estructuran generalmente en torno a los siguientes ejes temáticos: la seguridad y privacidad en las redes, el

desarrollo seguro de aplicaciones y la auditoría de seguridad de redes, servicios y sistemas. Estos conceptos están estrechamente vinculados con conocimientos previos en redes de datos, sistemas operativos y programación, y se orientan a diferentes aspectos de la seguridad informática. Sin embargo, cuando pensamos en introducir temas de ciberseguridad en la escuela secundaria, los conocimientos previos necesarios para comprenderlos, en general, son totalmente desconocidos. Es por ello que en este proyecto los contenidos se orientan a estudiantes sin conocimientos previos en computación y sin experiencia previa en competencias de seguridad informática [14, pp. 50-57]. En este sentido, los contenidos seleccionados abordan las temáticas descritas en la Tabla 1.

Tabla 1. Contenidos de ciberseguridad seleccionados para trabajar en la escuela

Tema	Contenido de ciberseguridad que se trabaja	Descripción	Objetivo de aprendizaje
Inteligencia de fuentes abiertas	Investigación y procesamiento de datos	La inteligencia de fuentes abiertas consiste en la recolección de datos de una persona o entidad que se encuentran disponibles de forma pública, junto con su posterior análisis y uso	Que los estudiantes realicen búsquedas avanzadas en la web para obtener resultados más precisos y puedan comprender la importancia de la privacidad de la información
Ingeniería Social	Fraudes	La ingeniería social consiste en engaños que realizan personas malintencionadas para hacer que su víctima entregue información confidencial, p. ej. datos bancarios	Que los estudiantes tomen conciencia respecto de las amenazas a las que se enfrentan en

Tema	Contenido de ciberseguridad que se trabaja	Descripción	Objetivo de aprendizaje
			la vida cotidiana al momento de utilizar los dispositivos tecnológicos
Criptografía	Confidencialidad y privacidad	La criptografía es una técnica que se usa para proteger información, que se basa en codificar un mensaje de manera que quede expresado de forma enigmática y así garantizar que sólo el destinatario legítimo pueda comprenderlo	Que los estudiantes se familiaricen con prácticas de ciberseguridad de uso conocido en Internet, p. ej. el protocolo HTTPS ² utilizado para acceder a páginas web cifrando la comunicación entre el cliente y el servidor de manera que si un tercero intercepta esa comunicación no puede comprenderla
Esteganografía	Confidencialidad y	Es una disciplina que trata sobre técnicas que	Que los estudiantes

² HTTPS es el acrónimo en inglés de Hypertext Transfer Protocol Secure. Es el protocolo de transferencia de datos utilizado para enviar datos entre un navegador web y un sitio web. HTTPS encripta los datos para aumentar la seguridad de las transferencias de datos.

Tema	Contenido de ciberseguridad que se trabaja	Descripción	Objetivo de aprendizaje
	privacidad	permiten ocultar mensajes u objetos (archivos) dentro de otros, llamados portadores (archivos multimedia de imágenes, audio o video), de modo que no se perciba su existencia. Los mensajes ocultos muchas veces son cifrados previamente, lo cual le otorga un nivel de seguridad extra	conozcan otras técnicas utilizadas para mantener la confidencialidad en una comunicación embebiendo un mensaje oculto por ejemplo en una foto o en un archivo de audio

Por otro lado, los contenidos elaborados para los distintos eventos CTF se desarrollaron teniendo en cuenta el contexto social de ese momento (COVID, virtualidad, mundial de fútbol, celebrities del momento, etc.) dando cuenta cómo personas malintencionadas sacan provecho de las preocupaciones e intereses sociales para engañar, ejecutar sus ataques y conseguir un resultado exitoso. Con ello, se busca desde el proyecto que los estudiantes comprendan que las amenazas se van adaptando a los contextos sociales y que para evaluar la seguridad e implementar controles también hay que tener en cuenta dicho contexto.

3 CTF en escuelas secundarias: una propuesta de cómo enseñar ciberseguridad

Se conoce como *Capture The Flag (CTF)* a eventos o competencias de Seguridad Informática cuya finalidad es fomentar el desarrollo y formación profesional en esta área de conocimiento, en un entorno estrechamente vinculado con lo lúdico, en donde la estrategia de aprendizaje se basa en la resolución de problemas de ciberseguridad, mediante el trabajo en equipo. Estas competencias se realizan en una plataforma virtual con característica de gamificación, es decir, con una dinámica propia de los juegos como la inclusión de reglas, interactividad, retroalimentación, niveles, recompensas, insignias, etc. Para [15] el aprendizaje basado en problemas es un

método de aprendizaje cuyo principio es el uso de problemas auténticos y complejos como punto de partida para la adquisición e integración de los nuevos conocimientos. Dicho autor señala de la siguiente manera las características fundamentales del aprendizaje basado en problemas: “El aprendizaje está centrado en el alumno; el aprendizaje se produce en pequeños grupos; los profesores son facilitadores o guías de este proceso; los problemas son el foco y estímulo para el aprendizaje; los problemas son un vehículo para el desarrollo de habilidades de resolución de problemas; la nueva información se adquiere a través del aprendizaje autodirigido”.

Por otro lado, los eventos CTFs constituyen una práctica comúnmente usada, tanto a nivel nacional como internacional, para la formación profesional en ciberseguridad y la promoción de comunidades en torno a este tema, ejemplo de ello son las Ekoparty³ y la DEFCON⁴ [16].

Para el desarrollo de los eventos CTFs se optó por la utilización de la herramienta CTFd⁵, dado que es un proyecto de código fuente abierto que ofrece la posibilidad de crear competencias de manera eficaz, y en la actualidad es adoptado ampliamente por la comunidad de ciberseguridad. La usabilidad, seguridad, portabilidad y la capacidad de generar estadísticas de las competencias (tanto de los equipos como de los usuarios) fueron los criterios que guiaron la elección de CTFd [14, pp. 30-54]. Dichas estadísticas resultaron de suma utilidad a la hora de evaluar el desempeño de los estudiantes, tanto en el momento en que se desarrolla la competencia (brindando un monitoreo en tiempo real y ayudas oportunas) como al finalizar la misma para hacer un análisis posterior.

De las modalidades existentes para el desarrollo de los CTFs se optó por la de tipo “jeopardy”, la cual se basa en desafíos que al resolverlos entrega un texto secreto denominado bandera o flag [17]. Este flag no es más que un texto en un formato específico, y el descubrirlo implica la resolución del desafío. Todos los desafíos poseen un puntaje y si uno de los participantes responde correctamente uno de ellos, el mismo se resuelve para todo su equipo, sumándole puntos al grupo y, si la respuesta es incorrecta, sólo se alerta al usuario que la misma no es válida (no se decrementan puntos ni se penaliza al equipo de ninguna manera). La cantidad de intentos para responder es ilimitada. A medida que un equipo resuelve desafíos, comienzan a habilitarse otros. Los desafíos se ordenan de acuerdo a un criterio de dificultad gradual, con la intención que los estudiantes puedan acceder a los conocimientos de manera progresiva. Dentro de los desafíos es posible acceder a ayudas que, en algunos casos se canjean por puntos (recurso comúnmente usado en la gamificación). El CTF tiene un horario de comienzo y uno de finalización y al llegar al final, el equipo

³ Ekoparty es una conferencia anual de ciberseguridad que, por sus características únicas y su particular estilo, se ha convertido en un referente para toda Latinoamérica. (<https://www.ekoparty.org>)

⁴ DEFCON es una de las conferencias de ciberseguridad más importantes que se desarrolla en Estados Unidos de manera anual (<https://defcon.org/>)

⁵ CTFd: <https://ctfd.io/>

ganador será el que acumule la mayor cantidad de puntos, y en caso de empate, el ganador es el que resolvió los ejercicios más rápidamente.

En relación a la puesta en acción de la plataforma “CTF en escuelas secundarias”, su diseño se orientó, como se describió previamente, a estudiantes sin conocimientos previos en computación y sin experiencia previa en competencias de seguridad informática. La adaptación de CTFd implementada en esta propuesta ofrece material didáctico, en formato de presentaciones, que incluye una breve explicación introductoria a las temáticas, con el objetivo de ofrecer orientaciones o ayudas a los estudiantes para la resolución de los desafíos. La idea de utilizar este material adicional es un aporte relevante a los CTF convencionales, en donde no se ofrece ningún tipo de orientación. En nuestro caso, el proceso de gamificación se logra adaptando la dinámica CTF a un juego con guías más completas, que faciliten el proceso de aprendizaje. Otro de los lineamientos de diseño de la plataforma “CTF en escuelas secundarias” fue concebir los desafíos para que puedan ser resueltos usando herramientas online (de acceso libre y disponibles en Internet) y evitar que los estudiantes tengan que instalarlas en sus computadoras.

4 Experiencias y aprendizajes

En la siguiente sección se describen y analizan las experiencias de los CTFs realizados en los últimos 5 años, dando cuenta de: a) la adaptación de los contenidos o desafíos al contexto, con la intención de mostrar la relación entre la ciberseguridad y las temas actuales (como podría ser la pandemia del covid19, las elecciones de gobierno en una jurisdicción o un evento deportivo); b) la modalidad adoptada y, c) la conformación de los equipos. A su vez, todas las experiencias son evaluadas mediante la administración de encuestas a los estudiantes y docentes. En la Tabla 2 se resumen las experiencias de “CTF en escuelas secundarias”.

Tabla 2. Sistematización de los eventos “CTF en escuelas secundarias”

Fecha	Modalidad	Duración	Escuelas	Edades	Participantes
18/10/2019	Presencial	1 hora y 20 minutos	ES N° 14 de La Plata, EEST N°5 de Villa Elvira (La Plata)	15 y 16 años	6 estudiantes y 1 profesora
13/11/2019	Presencial	3 horas y un recreo de 30'	Liceo “Víctor Mercante” (UNLP), ES N° 14 de La Plata, ES N° 50 de Tolosa	14 a 17 años	18 estudiantes

Fecha	Modalidad	Duración	Escuelas	Edades	Participantes
23/04/2020	Virtual	2 horas	EEST N°1 "Gral San Martín" de Berisso, EEST N°5 de Villa Elvira (La Plata), ES "Nuestra Señora del Valle" de La Plata	15 a 18 años	21 estudiantes
24/10/2020	Virtual	2 horas y 30 minutos	ES N° 50 de Tolosa, Estudiantes becados por la embajada de EEUU, Programa Space Camp	13 a 17 años	20 estudiantes y 5 profesores
30/10/2021	Virtual	3 horas	ES N° 31 de La Plata, ES N° 17 de La Plata, Liceo "Víctor Mercante" (UNLP)	13 a 17 años	4 estudiantes y 3 profesores
29/11/2022	Presencial	4 horas	EEST N°2 de Ensenada, EEST N°5 de Villa Elvira (La Plata), ES N° 14 de La Plata, Liceo "Víctor Mercante" (UNLP)	17 a 20 años	20 estudiantes y 6 profesores
22/11/2023	Presencial	4 horas	EEST N°2 de Berisso, ES N° 17 de La	15 a 17 años	40 estudiantes y 5 profesores

Fecha	Modalidad	Duración	Escuelas	Edades	Participantes
			Plata, EEST N° 2 de Ensenada, EEST N° 5 de Villa Elvira (La Plata)		

4.1 Etapa 1: los primeros CTF

Los primeros CTFs realizados en 2019 resultaron de suma utilidad para evaluar la herramienta y la percepción de estudiantes y docentes frente a contenidos nuevos y una estrategia de enseñanza no convencional basada en resolución de problemas y gamificación [18, pp. 58-60]. Estas experiencias resultaron valiosas en tanto permitieron realizar adaptaciones sobre los contenidos y la herramienta CTFd, por ejemplo ofreciendo ayudas que los estudiantes administraban de manera autónoma.

En relación a los contenidos, teniendo en cuenta la formación de los estudiantes, se optó por incluir desafíos sobre las temáticas descritas en la tabla 1. En las Figuras 1, 2, 3.a y 3.b se muestran ejemplos de los desafíos para las temáticas de Inteligencia de Fuentes Abiertas (OSINT), Ingeniería Social y Criptografía, utilizados en pasadas ediciones del CTF.

La modalidad adoptada fue presencial en las instalaciones de la Facultad de Informática y, en relación a la conformación de los equipos, en estas primeras experiencias facilitamos que los grupos fueran diversos en cuanto a edades. Con respecto a la participación de los docentes se les sugirió que (de manera opcional) ayuden o motiven a sus alumnos durante la competencia. Del primer CTF se aprendió que: a) la duración resultó escasa para los estudiantes, b) la complejidad de los desafíos respecto a la comprensión de las temáticas requirió de asistencia por parte de los organizadores y c) se presentó una barrera idiomática, dado que las herramientas utilizadas para la resolución se pueden encontrar fácilmente realizando búsquedas en Internet en inglés pero no resulta tan sencillo en español. Esta fue la motivación para incorporar ayudas (tanto para simplificar la búsqueda de herramientas como ofrecer materiales explicativos de los temas) favoreciendo una participación más autónoma. Por otro lado, proyectar la tabla de posiciones durante toda la competencia, ofrecer premios al equipo ganador y el acompañamiento por parte de los docentes, favoreció la motivación y el compromiso de los estudiantes.



Figura 1. Desafío sobre OSINT



Figura 2. Desafío sobre Ingeniería Social



Figura 3.a - Desafío sobre Criptografía: mensaje encriptado



Figura 3.b - Desafío sobre Criptografía: resultado de descryptar el mensaje

3.2 Etapa 2: CTF en pandemia COVID-19

En 2020 la realidad de la pandemia y el aislamiento social obligó a repensar los CTFs, no solo en el sentido de optar por la modalidad virtual, sino también en cómo adaptar la propuesta. Se tuvo que considerar que las escuelas con las que se trabaja desde el proyecto, en muchos casos son de barrios periféricos de La Plata, en donde las posibilidades de conexión a Internet desde los hogares de los estudiantes y de equipamiento disponible fue limitado [18, pp. 62].

En relación a los contenidos, los desafíos giraron en torno a las mismas temáticas, y se incluyeron imágenes explicativas o pistas que funcionaron como ayudas, facilitando la comprensión de los desafíos. La conformación de los equipos se mantuvo diversa, priorizando el gusto y posibilidades de las escuelas. En este punto, entendemos que ante una situación tan adversa como la pandemia y el aislamiento social, alentar la participación fue la condición prioritaria.

La primera competencia de esta etapa se desarrolló en el marco del día mundial de las “Mujeres en las TIC”. Para esta ocasión, se decidió relacionar el contenido a las

mujeres que contribuyeron al desarrollo de la Informática y de aquellas que actualmente se desempeñan en el campo de la ciberseguridad, incorporando desafíos con datos relevantes de libros, programas, proyectos o conferencias destacadas, en las que las referentes mujeres participaron. Por otra parte, en este evento se les dió más protagonismo a los docentes en su rol de acompañar a sus estudiantes.

El segundo CTF virtual contó con una dificultad extra para el equipo organizador: los jóvenes participantes provenían de dos mundos completamente diferentes. Por un lado estudiantes becados del “Programa Space Camp” de la Embajada de USA que concurren a escuelas de nuestro país distribuidas en diferentes lugares y por el otro estudiantes de una escuela de La Plata, caracterizada por pertenecer a una comunidad socialmente vulnerada. Esta diversidad nos planteó repensar la organización de los equipos: a) conformar grupos integrados por estudiantes de ambas instituciones y promover la colaboración; b) cada equipo tuvo asignado una sala de videollamada para que los estudiantes puedan organizarse y conocerse, un docente para el acompañamiento pedagógico y una persona del equipo organizador para evacuar dudas.

En el tercer CTF virtual participaron solo 4 estudiantes de 24 registrados, lo cual se debió a un corte de suministro eléctrico en gran parte de la ciudad de La Plata y alrededores. Ello dejó expuesta la diferencia de edades, dado que dos estudiantes tenían 17 años, uno 14 y otro 13, y los resultados dejaron en evidencia que los estudiantes más grandes contaban con más recursos para resolver los desafíos. La organización de los equipos fue por escuela y cada grupo tuvo asignado una sala de videollamada para facilitar la comunicación.

De la primera experiencia virtual se aprendió que, si bien la intención fue darle protagonismo a los docentes, el hecho que el docente actúe de intermediario en la comunicación complejizó la organización del evento. En este sentido, en las siguientes instancias, se decidió que los docentes mantengan un rol central como acompañantes pedagógicos. Es por ello que en la siguiente instancia virtual se habilitaron salas virtuales permitiendo que el equipo organizador estuviese más cerca de los estudiantes y resolver rápidamente cualquier inconveniente (ya sea técnico o conceptual).

La segunda experiencia virtual amplió las fronteras, favoreciendo la participación de estudiantes de diferentes provincias de la Argentina. Esta modalidad podría explotarse para hacer competencias entre diferentes jurisdicciones o regiones, creciendo así el alcance del proyecto y su impacto. Pero también se debe tener en cuenta los riesgos de hacerlo virtual, como la falla de las conectividades o del suministro eléctrico.

A partir de la tercera experiencia virtual comprendimos que el diseño de los CTFs debía contemplar las edades de los estudiantes, y en este sentido organizar eventos diferenciados para estudiantes del primer ciclo y segundo ciclo del nivel secundario.

3.3 Etapa 3: CTFs post pandemia COVID-19

En noviembre del 2022, recuperada la presencialidad, se realizó un CTF en modalidad presencial en la Facultad de Informática de la UNLP. En esta etapa, a partir de los aprendizajes previos, el evento se dirigió a estudiantes del segundo ciclo de la escuela secundaria. Los equipos se integraron con estudiantes de una escuela y uno o más docentes del establecimiento acompañando el proceso. Los organizadores se encontraban en la misma aula para evacuar todo tipo de dudas y consultas. En esta última instancia, los docentes tuvieron un rol fundamental dado que ayudaron a sus estudiantes a organizarse para poder emprender en grupo la resolución de los desafíos.

Esta experiencia fue una de las más enriquecedoras, dado que finalizada la competencia los estudiantes propusieron quedarse realizar una revisión de las soluciones a los desafíos que no pudieron resolver e hicieron preguntas sobre cómo inscribirse en la Universidad. Consideramos que la participación de estudiantes próximos a egresar de la escuela secundaria y la vuelta a la presencialidad en la facultad fueron factores claves en la realización de este CTF.

De acuerdo con el resultado de las encuestas administradas al finalizar el CTF del 2022 el 93% de los estudiantes consideró que la plataforma les resultó fácil de utilizar, lo cual es relevante dado que para el 71% fue su primera experiencia participando en un CTF. Según las respuestas obtenidas, las categorías en las cuales resolvieron mayor cantidad de desafíos fueron inteligencia de fuentes abiertas y criptografía. El 85% consideró que el tiempo de duración del evento fue suficiente. De las respuestas a las preguntas abiertas, se destaca el hecho que consideraron que los desafíos los hacían pensar de manera diferente y que la competencia fue motivante. Además, hicieron hincapié en que se divirtieron y que aprendieron jugando. Un dato interesante es que para el 86% el trabajo en equipo influyó positivamente en los resultados del grupo y destacan que se ayudaban entre sí para resolver los desafíos. Por último, todos los encuestados manifiestan que les gustaría volver a participar.

En esta experiencia se realizaron por primera vez encuestas a los docentes dado que es interés del equipo de trabajo conocer la mirada docente acerca de la actividad; las mismas arrojaron los siguientes datos: a) todos los docentes encuestados manifestaron que la plataforma fue sencilla de utilizar, los desafíos les resultaron de un nivel intermedio de complejidad, el tiempo de duración de la competencia les resultó suficiente y que el trabajo en equipo es una metodología que aplican de forma cotidiana en el aula; b) algunos docentes indicaron que trabajan con las temáticas de criptografía e ingeniería social en sus clases; c) todos los docentes consideran positivo implementar una competencia tipo CTF adaptado a temas específicos que se trabajan en la escuela, porque colabora a la comprensión y la apropiación de los contenidos; d) la mayoría de los docentes considera adecuado realizar una competencia CTF sobre ciberseguridad con estudiantes del ciclo básico, con un menor nivel de complejidad de los desafíos, lo cual coincide con nuestra visión, a partir de la experiencia acumulada en el proyecto, organizando CTFs por edades. Por último, en relación a la pregunta sobre el aporte de la actividad a la formación de los estudiantes, algunas citas de los docentes resultan elocuentes: “Es una experiencia distinta a la que están

acostumbrados, debían coordinar y apoyarse mutuamente eso les sirve para reforzar lo que es el trabajo en equipo.”, “Acentuó la importancia de leer bien los enunciados y de buscar información antes de preguntarle al docente. Contribuyó al desarrollo de uno de los pilares de la educación: aprender a aprender”, “Creo que es una actividad que desafió a los estudiantes, les permitió usar herramientas que les eran desconocidas, les despertó el interés sobre temáticas que nunca habían abordado. El trabajo en equipo los potenció.”

3.4 Etapa 4: accesibilizar CTFd para CTFs en escuelas

En noviembre del 2023, se organizó un nuevo CTF en modalidad presencial en la Facultad de Informática de la UNLP. En esta edición se incorporaron al equipo de trabajo un tesista de Licenciatura en Sistemas, quien se encuentra desarrollando su tesis de grado en el marco del proyecto de “Extensión en Vínculos con Escuelas Secundarias”, y tres estudiantes de las carreras de la Facultad interesados en integrar el proyecto.

A pesar de disponer de una instancia de la herramienta CTFd adaptada para las competencias de ciberseguridad con escuelas secundarias, las diferentes ediciones realizadas del evento permitieron dar cuenta de las debilidades de la herramienta, fundamentalmente desde el punto de vista de la creación, configuración de eventos y carga de desafíos, entre otras tareas, requiriendo esfuerzo extra en el equipo de trabajo con tareas factibles de automatizar. Algunas de las debilidades de la plataforma CTFd se hacen evidentes en ciertos procesos, entre ellos:

- a) la carga de desafíos: requiere ser realizada manualmente a través de la interfaz de usuario, careciendo de una opción automatizada para un usuario final, por ejemplo un docente de una escuela;
- b) la unión de los estudiantes a los equipos: requiere que el estudiante memorice el nombre del equipo y su contraseña, acción frecuentemente proclive a errores de tipeo que ocasiona retrasos al inicio de la competencia.

La automatización de éstas y otras tareas mejorarían la experiencia de los diferentes usuarios de la herramienta tanto autores como jugadores. La tesina de grado mencionada previamente aborda este problema y tiene por objetivo automatizar y mejorar la plataforma, y la experiencia de usuario, en el sentido que resulte más accesible para los docentes, estudiantes y autores (generadores de contenido), al momento de organizar y participar en la competencia.

Uno de los objetivos de este evento fue identificar las tareas que se realizan mediante la interacción con la herramienta, factibles de mejorar, además de las ya relevadas a partir de las múltiples ediciones previas de los CTF. Disponer de una versión de CTFd personalizada para escuelas secundarias, que mejore la experiencia de usuario en el sentido analizado, permitiría por un lado, contribuir a la comunidad de CTFd y por otro, poner a disposición una versión de la herramienta para las escuelas que favorezca la realización de sus propios eventos CTF, promoviendo la apropiación de dicha herramienta.

En relación a los contenidos, los temas trabajados fueron los mismos y se agregó un desafío de esteganografía con un archivo de audio, para mostrar que es posible ocultar información en distintos tipos de objetos multimedia de manera que resulte imperceptible para el usuario. Por otro lado, la emergencia de las IA generativas al alcance de un click y el uso cotidiano que los jóvenes hacen de estas herramientas, motivó reflexiones sobre si los desafíos resultaban un reto para los estudiantes o si podían resolverse fácilmente con herramientas de IA. En este sentido, se intentó resolver los desafíos con ChatGPT y se llegó a la conclusión que las respuestas obtenidas eran imprecisas y en algunos casos erróneas. En relación a ello, los datos obtenidos de la encuesta administrada a los estudiantes nos permiten afirmar que, el 60% de los estudiantes utilizaron alguna herramienta de IA para resolver los desafíos, en este sentido nuestra hipótesis se comprobó, sin embargo un 30% de los mismos respondió que no le resultó útil y el otro 30% que solo lo fue para obtener “alguna respuesta”. Por otro lado, se observó, a partir de la misma encuesta, que el 22% de los estudiantes no usó ChatGPT por no estar familiarizados con el uso cotidiano de esta herramienta. Sin embargo, aunque el 60% de los estudiantes hicieron uso de ChatGPT, para el 75% de los mismos los desafíos resultaron de complejidad intermedia o alta. Por otra parte, el 100% de los docentes encuestados coincidieron en que la complejidad de los desafíos propuestos eran de un nivel intermedio para el nivel educativo de los alumnos.

Este CTF fue el más concurrido, dado que participaron 40 alumnos y 5 profesores, como se describe en la Tabla 2. La tarea de registrarse manualmente e iniciar sesión en la plataforma, obligó a invertir una cuarta parte del tiempo del CTF en la registración de los equipos. Ello evidenció que para que el proyecto escale y permita la participación de una mayor cantidad de estudiantes se torna esencial la automatización de estas tareas para agilizar la actividad y mantener el entusiasmo de los estudiantes. Además, la organización del evento se ve impactada por el aumento de escala en la cantidad de estudiantes y docentes dado que no solo hay que tener en cuenta la asistencia a los estudiantes en la resolución de los desafíos y acceso a la plataforma, sino también el trabajo previo que implica la preparación del espacio, las computadoras y materiales en general. Por este motivo, los estudiantes colaboradores desempeñaron un rol fundamental en las tareas de organización.

De acuerdo con el resultado de las encuestas administradas al finalizar el CTF del 2023: a) el 83,3% de los estudiantes consideró que la plataforma les resultó fácil de utilizar; b) para el 100% de los encuestados fue su primera experiencia participando en un CTF; c) las categorías en las cuales resolvieron mayor cantidad de desafíos fueron inteligencia de fuentes abiertas y criptografía; d) el 66,7% consideró que el tiempo de duración del evento fue suficiente; e) para el 88,9% de los estudiantes y el 100% de los docentes evaluó que el trabajo en equipo influyó positivamente en los resultados del grupo, les permitió distribuirse las tareas, coordinar las resoluciones y trabajar en equipo; f) todos los estudiantes y los docentes manifestaron que les gustaría volver a participar en otro CTF.

5 Conclusiones

La realización de los diferentes eventos CTF, en sus diferentes modalidades y diversidad de estudiantes, permitió observar la receptividad e interés de los jóvenes al interiorizarse sobre saberes técnicos del campo de la Informática, específicamente de ciberseguridad, así como también sobre saberes transversales vinculados con la comunicación, la organización y el trabajo colaborativo para poder alcanzar una meta común. En este sentido, a partir de las experiencias podemos afirmar que es posible realizar eventos “CTF en la escuela secundaria” en modalidad presencial y virtual, y que el rol docente como acompañante pedagógico, es fundamental tanto para alentar la participación como la resolución de los desafíos.

De la información relevada a partir de las encuestas a estudiantes y docentes, podemos concluir que adquirir conocimientos nuevos en forma activa, a través de la propia experimentación, realizando conjeturas, investigando y trabajando colaborativamente, resulta motivador y favorece la apropiación de los mismos dado que se adquieren en contextos y situaciones reales y cotidianas.

La adaptación a la virtualidad extendió las fronteras de los “CTF en escuelas secundarias” favoreciendo la participación de escuelas de diferentes provincias de la Argentina. Esto permite proyectar la formación de una red de aprendizaje en ciberseguridad en la escuela secundaria que aliente la participación de jóvenes, promueva vocaciones tecnológicas en seguridad informática (como campo específico dentro de la disciplina Informática) y consolide la articulación entre la escuela y la universidad pública.

Disponer de materiales educativos adecuados y pertinentes, como la plataforma “CTF en escuelas secundarias” utilizada en las experiencias presentadas en este trabajo, puede resultar un recurso didáctico útil a la hora de incluir a la ciberseguridad en los programas de las currículas de la escuela secundaria. Sin embargo, la portabilidad de la herramienta en el sentido de poder ser utilizada en las escuelas, en forma autónoma, requiere de ciertas mejoras de CTFd que atiendan la accesibilidad y la experiencia de usuario. Es esta línea en la que se encuentra trabajando el equipo del proyecto.

Referencias

1. Guichard J. (2002). Problemáticas y finalidades de la orientación profesional. En Revista Europea de Formación Profesional Núm. 26 Pág. 5-20.
2. Oliveros O. and González Bello J. (2012). Hacia un nuevo paradigma en orientación vocacional. *Paradigma*, 33(2), 127-141. Recuperado el 06 de abril de 2023, de http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1011-22512012000200007&lng=es&tlng=es.
3. Levis D. (2007). Enseñar y aprender con informática/ enseñar y aprender informática. Medios informáticos en la escuela argentina. En Cabello, R. y Levis D., eds. (2007)

- Tecnologías informáticas en la educación a principios del siglo XXI Buenos Aires: Prometeo.
4. ISACA (2020). Definición de ciberseguridad y su riesgo. Recuperado el 3 de mayo de 2023. <https://www.esic.edu/rethink/tecnologia/definicion-ciberseguridad-riesgo>.
 5. Advancing Computing as a Science & Profession. Curricula Recommendations. ACM-<https://www.acm.org/education/curricula-recommendations>
 6. Chen, W., He, Y., Tian, X., and He, W. (2021). Exploring cybersecurity education at the K-12 level. In E. Langran & D. Rutledge (Eds.), Proceedings of SITE Interactive Conference (pp. 108-114). Association for the Advancement of Computing in Education.
 7. Paller A. (2017). Inspiring the next generation of cybersecurity experts. Sans. Cyberstar. Recuperado el 24 de abril de 2023, de <https://www.sans.org/media/cyberstart/Virginia-CyberStart-Report.pdf>
 8. OEA (2023). Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades. Recuperado el 20 de abril de 2023, de: https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf
 9. (ISC)2 Cybersecurity Workforce Study (2022). Recuperado el 24 de abril de 2023, de <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx>.
 10. Deterding S., Dixon D., Khaled R. and Nacke L. (2011). From game design elements to gamefulness: defining "gamification". In Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments (MindTrek '11). Association for Computing Machinery, New York, NY, USA, 9–15.
 11. Gallego-Durán F., Molina-Carmona R., and Llorens Largo, F. (2014). Gamificar una propuesta docente. Diseñando experiencias positivas de aprendizaje.
 12. Leune K. and Petrilli S. (2017). Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. SIGITE '17: Proceedings of the 18th Annual Conference on Information Technology Education. September 2017. pp. 47–52.
 13. Geelan, Ben & de Salas, Kristy & Lewis, Ian & King, Carolyn & Edwards, Dale & mara, Aidan. (2015). Improving Learning Experiences Through Gamification: A Case Study. Australian Educational Computing. 30.
 14. Suárez G., Bolino P. (2020). "Capture the Flag" aplicada a la enseñanza de Ciberseguridad en escuelas. Sedici. <http://sedici.unlp.edu.ar/handle/10915/118187>
 15. Barrows, H. (1986). Taxonomy of problem-based learning methods. Medical education: 20(6). <http://dx.doi.org/10.1111/j.1365-2923.1986.tb01386.x>
 16. Díaz, J., Venosa, P., Macia, N., Lanfranco, E., Sabolansky, A., Durante, M., Rubio, D. Pretto, J. (2020). Participación y despliegue de CTFs como herramienta para fortalecer la formación en ciberseguridad. XXII Workshop de Investigadores en Ciencias de la Computación. <http://sedici.unlp.edu.ar/handle/10915/104050>
 17. CTFtime team. (s.f.). What is Capture The Flag?. Ctfime. <https://ctftime.org/ctf-wtf/>.
 18. Suárez G., Bolino P., Pretto J., Venosa P. y Queiruga C. (2021). CTFs en escuelas: una plataforma para acercar la ciberseguridad a la educación secundaria. Actas de las Primeras Jornadas Argentinas de Didáctica de Ciencias de la Computación: JADiCC 2021. Ciudad Autónoma de Buenos Aires, Fundación Sadosky. ISBN 978-987-27416-9-3.